UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,706	09/29/2003	Hye-Sook Hwang	0630-1851P	9257

2292 7590 06/12/2009

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
ALI, FARHAD	

ART UNIT	PAPER NUMBER
2446	

NOTIFICATION DATE	DELIVERY MODE
06/12/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/671,706	HWANG, HYE-SOOK	
	Examiner	Art Unit	
	FARHAD ALI	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 15-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 15-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims:

Claims 1-13 and 15-20 are pending in this Office Action.

Claims 1, 6 and 17 are amended.

Claims 18-20 are new

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/18/2009 has been entered.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zintel (US 6,779,004 B1) in view of Slaughter et al. (US 6,970,869 B1), hereinafter Slaughter.

Claim 1

Zintel teaches a selective device recognition apparatus in a UPnP based home network, the apparatus comprising: a network stream processing unit configured to parse a device characteristic data of a device and to read a network transmission possible identifier and a device characteristic identifier, the device being automatically detectable in the UPnP based home network **(Column 7 Lines 8-23 "User Control Point" and "The set of modules that enable communication with a UPnP Controlled Device..."; and see Table on column 14 "Description Client" which "receive description documents")**.

Zintel does not specifically disclose wherein the network transmission possible identifier is set to recognize a device according to a user's authority; and a network transmission judging unit configured to compare the read network transmission possible identifier with a preset network transmission possible identifier recorded in a transmission judgment table, to judge whether to perform network transmission of the device characteristic data according to a result of the comparison, and to transmit the device characteristic data only when the network transmission possible identifier read from the network stream processing unit is matched with the present network transmission possible identifier recorded in the transmission judgment table.

Slaughter teaches in Column 7 lines 42-57, "Service providers (or a listener agent) may respond to search requests by publishing or providing corresponding advertisements or URIs to corresponding advertisements. When a service provider responds to a discovery search request (either directly or through a listener agent), the

provider may choose to publish a protected or an un-protected (complete) advertisement. A protected advertisement may include the set of information necessary to obtain a complete advertisement. Publishing a protected advertisement, forces the client to the obtain a valid credential from an authentication service before receiving the complete un-protected advertisement from the service provider. A complete un-protected advertisement is needed to create a gate, and therefore to use the service" and in Column 53 lines 46-63, "In some embodiments, a mechanism for verifying that a client attempting to run a service, for verifying that the service advertisement received by the client is an authorized service advertisement, and for verifying that the space from which the client received the service advertisement is authorized may be based upon a public key/private key asymmetric cryptographic mechanism. In this mechanism, an authorized sending entity may embed a public key in a message and encrypt the message including the public key with its private key. An entity receiving the encrypted message may decrypt the message using the public key and find the same public key embedded in the decrypted message, and thus verify that the message is from the authorized entity, since only that entity has the private key necessary to encrypt the message" in order to "provide an additional level of security for the service provider" (Column 7 lines 58-60).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Zintel to include "Service providers (or a listener agent) may respond to search requests by publishing or providing corresponding advertisements or URIs to corresponding advertisements. When a service provider

responds to a discovery search request (either directly or through a listener agent), the provider may choose to publish a protected or an un-protected (complete) advertisement. A protected advertisement may include the set of information necessary to obtain a complete advertisement. Publishing a protected advertisement, forces the client to the obtain a valid credential from an authentication service before receiving the complete un-protected advertisement from the service provider. A complete un-protected advertisement is needed to create a gate, and therefore to use the service" and "a mechanism for verifying that a client attempting to run a service" as taught by Slaughter in order to "provide an additional level of security for the service provider" (Column 7 lines 58-60).

Claim 2

Zintel teaches the apparatus of claim 1, further comprising:

a network interface configured to receive the device characteristic data transmitted from a home network device **(Column 7 Lines 8-23 "User Control Point" and "The set of modules that enable communication with a UPnP Controlled Device…")**.

Claim 3

Zintel teaches the apparatus of claim 1, wherein the network stream processing unit includes:

a preprocessor configured to parse the device characteristic data;

a buffer manager configured to temporally store the device characteristic data parsed in the preprocessor in a buffer and to output a registry signal corresponded thereto;

and an identifier reader configured to search the device characteristic data temporally stored in the buffer according to the registry signal outputted from the buffer manager and read the device characteristic identifier and the network transmission identifier **(See Figure 21. "Processing Unit" "RAM" "LAN" and "Applications").**

Claim 4

Zintel teaches the apparatus of claim 3, wherein the preprocessor performs parsing of the device characteristic data by device characteristic data units divided by a token(/) **(See Figure 16 XML data in token format)**.

Claim 5

Zintel teaches the apparatus of claim 1, wherein the network transmission judging unit includes:

a device characteristic identifier detecting module configured to detect a device characteristic identifier that is the same with the device characteristic identifier read from the network stream processing unit;

a network transmission possible identifier comparing module configured to compare the network transmission possible identifier detected by the device

characteristic identifier detecting module with the network transmission possible identifier read from the network stream processing unit; and

a transmission judging module configured to judge whether it is possible to perform the network transmission of the device characteristic data indicated by the device characteristic identifier according to the comparison result **(Column 11 Lines14-15 "Discovery Client" is "The module that runs in a User Control Point that initiates SSDP queries" and Column 14 Line 9 "Description Client" and see Figure on column 14 "Description Client" which "receive description documents" and Column 7 Lines 8-23 "User Control Point" and "The set of modules that enable communication with a UPnP Controlled Device...")**.

Claim 6

Zintel teaches a selective device recognition method in a UPnP based home network, the method comprising:

receiving and parsing a device characteristic data of a device, the device being automatically detectable in the UPnP based home network **(see Figure on column 14 "Description Client" which "receive description documents")**;

reading a device characteristic identifier and a network transmission possible identifier from the parsed device characteristic data **(Column 11 Lines14-15 "Discovery Client" is "The module that runs in a User Control Point that initiates SSDP queries" and Column 9 Lines 6-8 "Description Document" "A structured**

unit of data that is used by a User Control Point or UPnP Bridge to learn the capabilities of a Controlled Device").

Zintel does not specifically disclose wherein the network transmission possible identifier is set to recognize a device according to a user's authority; and comparing the read network transmission possible identifier with a preset network transmission possible identifier recorded in a transmission judgment table, judging whether to perform network transmission of the device characteristic data corresponded to the read device characteristic identifier is performed according to a result of the comparison, and transmitting the device characteristic data only when the read network transmission possible identifier is matched with the preset network transmission possible identifier recorded in the transmission judgment table.

Slaughter teaches in Column 7 lines 42-57, "Service providers (or a listener agent) may respond to search requests by publishing or providing corresponding advertisements or URIs to corresponding advertisements. When a service provider responds to a discovery search request (either directly or through a listener agent), the provider may choose to publish a protected or an un-protected (complete) advertisement. A protected advertisement may include the set of information necessary to obtain a complete advertisement. Publishing a protected advertisement, forces the client to the obtain a valid credential from an authentication service before receiving the complete un-protected advertisement from the service provider. A complete un-protected advertisement is needed to create a gate, and therefore to use the service" and in Column 53 lines 46-63, "In some embodiments, a mechanism for verifying that a

client attempting to run a service, for verifying that the service advertisement received by the client is an authorized service advertisement, and for verifying that the space from which the client received the service advertisement is authorized may be based upon a public key/private key asymmetric cryptographic mechanism. In this mechanism, an authorized sending entity may embed a public key in a message and encrypt the message including the public key with its private key. An entity receiving the encrypted message may decrypt the message using the public key and find the same public key embedded in the decrypted message, and thus verify that the message is from the authorized entity, since only that entity has the private key necessary to encrypt the message" in order to "provide an additional level of security for the service provider" (Column 7 lines 58-60).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Zintel to include "Service providers (or a listener agent) may respond to search requests by publishing or providing corresponding advertisements or URIs to corresponding advertisements. When a service provider responds to a discovery search request (either directly or through a listener agent), the provider may choose to publish a protected or an un-protected (complete) advertisement. A protected advertisement may include the set of information necessary to obtain a complete advertisement. Publishing a protected advertisement, forces the client to the obtain a valid credential from an authentication service before receiving the complete un-protected advertisement from the service provider. A complete un-protected advertisement is needed to create a gate, and therefore to use the service"

and "a mechanism for verifying that a client attempting to run a service" as taught by Slaughter in order to "provide an additional level of security for the service provider" (Column 7 lines 58-60).

Claim 7

Zintel teaches the method of claim 6, wherein parsing the received device characteristic data is performed by device characteristic data units divided by a token(/) or parsing the received device characteristic data is performed by inserting a null string after the token in the parsing step **(Column 33 Lines 36-42 "SzHeaders [in] null-terminated text string containing the headers for the event, each separated by CRLF. SzEventBody [in] null-terminated text string containing the body of the event message")**.

Claim 8

Zintel teaches the method of claim 6, wherein the device characteristic data is a request message for UPnP device recognition in a UPnP CP (control point) device **(Column 11 Lines14-15 "Discovery Client" is "The module that runs in a User Control Point that initiates SSDP queries")**.

Claim 9

Zintel teaches the method of claim 8, wherein the request message includes inherent network transmission possible identifier information per each device characteristic identifier **(Applicant admits inherency in the claim).**

Claim 10

Zintel teaches the method of claim 8, wherein the UPnP device includes the network transmission possible identifier, and recognition is judged by the UPnP CP device **(See Figure 10 and see Table on column 14 "Discovery Client" "Discovery Server" "Description Client" "Description Server" and "Control Server")**.

Claim 11

Zintel teaches the method of claim 8, wherein the UPnP CP device and the UPnP device exist in a same local network **(See Figure 2 User Control Point and Controlled Device).**

Claim 12

Zintel teaches the method of claim 6, wherein the device characteristic data is an advertisement message for notifying a UPnP device itself **(see Figure on column 14 "Description Server" which "Provide description documents").**

Claim 13

Zintel teaches the method of claim 12, wherein the advertisement message includes inherent network transmission possible identifier information per each device characteristic identifier **(Applicant admits inherency in the claim)**.

Claim 15

Zintel teaches the method of claim 6, wherein the network transmission judging step includes:

outputting a request message to a UPnP CP (control point) device for a message not having network transmission possible identifier information;

and sequentially comparing each network transmission possible identifier with each network transmission possible identifier of a UPnP device for a message having network transmission possible identifier information and transmitting a response message to the UPnP CP device according to the comparison result **(Column 21 Lines 5-14 "User Control Points 104 are not required to have any prior knowledge of the SCPs 402 required to control the Services on the various devices. Therefore, a Controlled Device or Bridge must be able to describe to a User Control Point the protocols required to control its Services, such that the User Control Point will be able to implement these protocols dynamically")**.

Claim 16

Zintel teaches the method of claim 6, wherein the network transmission judging step includes:

recognizing a UPnP device by a general recognition process for a message not having the network transmission possible identifier information; and

sequentially the comparing network transmission possible identifier information with a network transmission possible identifier of a UPnP CP device when the network transmission possible identifier information is detected and recognizing a pertinent device and a service according to the comparison result **(Column 21 Lines 5-14 "User Control Points 104 are not required to have any prior knowledge of the SCPs 402 required to control the Services on the various devices. Therefore, a Controlled Device or Bridge must be able to describe to a User Control Point the protocols required to control its Services, such that the User Control Point will be able to implement these protocols dynamically")**.

Claim 17

Claim 17 is similar to scope of claims 1 and 6 and is rejected similarly to the reasons discussed above.

Claim 18

The apparatus of claim 1, wherein the network stream processing unit is configured to transmit a disable signal for intercepting a transmission of the device characteristic data only when the network transmission possible identifier and the preset network transmission possible identifier are different (See claim 1 rejection; The security

mechanism as taught by Slaughter wherein the key is not the proper key, would result in the device characteristic data not being sent).

Claim 19

The method of claim 6, further comprising: transmitting a disable signal for intercepting a transmission of the device characteristic data only when the network transmission possible identifier and the preset network transmission possible identifier are different (See claim 6 rejection; The security mechanism as taught by Slaughter wherein the key is not the proper key, would result in the device characteristic data not being sent).

Claim 20

The apparatus of claim 17, wherein the network stream processing unit is configured to transmit a disable signal for intercepting a transmission of the device characteristic data only when the network transmission possible identifier and the preset network transmission possible identifier are different (See claim 17 rejection; The security mechanism as taught by Slaughter wherein the key is not the proper key, would result in the device characteristic data not being sent).

Response to Arguments

3. Applicant's arguments filed 05/18/2209 have been fully considered but they are not persuasive.

In regards to the applicants arguments that Zintel in view of Slaughter does not teach that a user's authority is used to set to recognize a device, the examiner respectfully disagrees. Slaughter teaches in Column 53 lines 46-63, "In some embodiments, a mechanism for verifying that a client attempting to run a service, for verifying that the service advertisement received by the client is an authorized service advertisement, and for verifying that the space from which the client received the service advertisement is authorized may be based upon a public key/private key asymmetric cryptographic mechanism. In this mechanism, an authorized sending entity may embed a public key in a message and encrypt the message including the public key with its private key. An entity receiving the encrypted message may decrypt the message using the public key and find the same public key embedded in the decrypted message, and thus verify that the message is from the authorized entity, since only that entity has the private key necessary to encrypt the message". The examiner asserts that the user's authority is analogous to a security mechanism as taught by Slaughter, and furthermore in regards to the teaching of a disable signal, the security mechanism as taught by Slaughter wherein the key is not the proper key, would result in the device characteristic data not being sent.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FARHAD ALI whose telephone number is (571)270-

1920. The examiner can normally be reached on Monday thru Friday, 7:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Farhad Ali/
Examiner, Art Unit 2446

/Jeffrey Pwu/
Supervisory Patent Examiner, Art Unit 2446